UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,772	07/21/2000	Raynold M. Kahn	PD-200045	3987

20991 7590 01/22/2007
THE DIRECTV GROUP INC
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 09/620,772	**Applicant(s)** KAHN ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-29 and 31-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-29 and 31-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *1 September 2006*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 1 November 2006, with acknowledgement of an original application filed on 21 July 2000.

2. Claims 1, 2, 4-29, and 31-50 are pending claims 1, 17, and 28 are independent claims. Claim 1 is amended. Amendments to the claim and specification are accepted.

3. The IDS submitted 1 September 2006 has been considered.

4. The objections to the claims and specification are removed due to amendment and arguments submitted.

Response to Arguments

5. Applicant's arguments with respect to 1, 4-28, and 31-50 have been considered but they are not persuasive.

In response to Applicant's argument beginning on page 14 and stated beginning on page 18, "The Office Action acknowledges that the Okabe reference does not disclose the step of (e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key, but argues … The Applicants respectfully disagree that the Okabe reference discloses the features of claim 1 …

(A) Since Okabe does not disclose re-encrypting the program material with a second key at all (it does note disclose step (d) …

(B) The Office Action assert that Okabe discloses that "each time the transfer generation number, and the encryption resultant playback key data are updated, another key is generated", but the Applicants can find no part of Okabe that discloses this feature …

(C) Okabe, in fact, teaches away from such a modification, because the "encryption resultant contents data" remains is never "re-encrypted" .. not by the terminal, not by the first player, nor by the second player".

The Examiner disagrees with arguments presented and first, summarizes the rejection below to indicate that there is no difference in the understood meaning between 'encrypting a second key to produce a third' and 'encrypting a third key to produce a fourth'. Second the Examiner disagrees with argument (A) and notes that the player generates other second encryption resultant playback key data, the generating of this second or third encryption resultant playback key data has the same meaning as 're-encrypting'. Third in response to argument (B), the Examiner finds that Okabe discloses generating 'encrypted resultant content' each time material is distributed. The number of the key used for encryption/decryption is obviously incremented each time the encryption resultant playback key is generated, i.e. second or third. In response to Applicant's argument (C), the Examiner as stated in response to argument (A) the produced 'secondary encrypted resultant content' or 'third encrypted resultant content' has the same meaning as re-encrypting.

In response to Applicant's argument beginning on page 15, "(a) accepting encrypting access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data; Which the Office Action appears to analogize to the first player terminal apparatus receiving the primary encryption resultant playback key data and the encryption resultant content data". The Examiner notes, the Okabe reference teaches 'The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data'. The control information, the control information is interpreted to have the same meaning as 'the encryption resultant contents data' in the Okabe reference. Note the Okabe reference uses the terms 'encryption resultant playback key' and 'encryption resultant content data'. The control information is contained in the header of the encryption resultant content data header, see Okabe col. 8, lines 27-45.

In response to Applicant's argument beginning on page 16, "Claim 1 then recites the step of: (b) decrypting the receiving access control information in a conditional access module realeasble coupleable with the receiver to produce the first encryption key Which the Office Action indicates is disclosed by the first player … This is incorrect. The foregoing only discloses that the player recovers original contents data by decrypting it. It does not disclose the step of decrypting the received access control information in a conditional access module to produce the first encryption key". The Examiner disagrees this is clearly shown in Okabe see col. 7, lines 13-38, which teach how material is received by a player. The material received is the content as well as control data, which is interpreted to be equivalent to the 'encryption resultant data' in Okabe. The module further is able to copy the data according to the decrypted resultant data, i.e. control data.

In response to Applicant's argument beginning on page 16, "Claim 1 then recites the step of (c) decrypting the program material using the first encryption key; The Office Action indicates that this is disclosed as follows … The foregoing indicates that the original content data is recovered by decryption, but it does not indicate which key is used to accomplish this feat". The Examiner disagrees with argument and notes that Okabe clearly shows that the data distributed to the player is the encryption key as well as the encryption resultant content data. The encryption resultant playback key is used to decrypt the data.

In response to Applicant's argument beginning on page 17, "Claim 1, next recites: (d) re-encrypting the program material according to a second encryption key ... Analogizing this step to operations performed in player 6a, the Office Action indicates this is disclosed in Okabe as follows: ... This is incorrect. At no point does player 6a re-encrypt program material at all, nor does it do it so with a second key different than the key by which it was encrypted when it was received by the player 6a". The Examiner disagrees with argument and notes, that a second encryption resultant content data are generated, this has the same meaning as 're-encrypting'.

In response to Applicant's arguments beginning on page 19, with respect to claims 15 and 41 these arguments are moot due the new rejection below in which Akins clearly shows that the content data can contain time limitations as to how long distributed content can be viewed in col. 28, line 43 through col. 29, line 39.

In response to Applicant's arguments beginning on page 20, with respect to claim 17, these arguments are moot due the new rejection below in which Akins clearly shows that the content data can contain time limitations, i.e. temporally-variant control data as to how long distributed content can be viewed in col. 28, line 43 through col. 29, line 39.

In response to Applicant's argument on page 21, "Further as described above, Okabe does not disclose anything equivalent to a second encryption key (because it does not decrypt the media program and re-encrypt it ... the second player passes the encrypted program material to the second player in the same form as it received". The Examiner disagrees, and notes that

Okabe teaches that the player produces secondary encrypted resultant content, the encrypted resultant content, is the program re-encrypted.

In response to Applicant's argument on page 21, "Finally, Okabe does not disclose anything like a second decryption module for decrypting the fourth encryption key to produce the second encryption key". The Examiner disagrees and notes that the numbering of the keys is irrelevant, Okabe teaches separating encrypted resultant content to produce playback keys.

In response to Applicant's argument on page 21 with respect to claim 18, "As described above, Okabe does not disclose a second encryption module for re-encrypting the decrypted program material". The Examiner disagrees Okabe shows re-encrypting program material according to subsequent keys, the 'fourth' key is interpreted to be equivalent to second or third keys.

In response to Applicant's argument beginning on page 21 with respect to claim 25, "Claim 25 recites that the second encryption key is stored in the conditional access module. The Office Action suggest that this is disclosed as follows: ... but nothing in the foregoing discloses the use of a second encryption key for re-encrypting the decrypted program". The Examiner disagrees with argument and notes that Okabe teaches a second key is generated with the second encrypted resultant content, this content is stored.

In response to Applicant's argument beginning on page 22 with respect to claim 4, the Office Action has analogized the "player" of the Okabe reference to a "conditional access module" and the "receiver as the terminal. In rejecting claim 4, the Office Action now argues that it would be obvious that the "player" be a smartcard". The Examiner is confused by Applicant's interpretation and disagrees with argument. Claim 4 indicates "wherein the conditional access module is implemented on a smartcard". The player in Okabe obviously incorporates a computer terminal, the use of smartcards with computer terminals to assist with rights management is well known in the art. In addition Akins teaches the use of 'smartcards' with the cable television system, in which digital data is distributed.

In response to Applicant's argument on page 23 with respect to claim 5, "The Office Action suggests that the foregoing discloses that the access control information includes metadata describing at least one right for the program material ... In fact, the foregoing discloses the opposite. It discloses that access control information is stored in the set top box, not in metadata transmitted with the access control information". The Examiner disagrees with argument for multiple reasons, notes that both references as whole should be interpreted for the rejection of the claims, and again is confused by Applicant's interpretation. The passage indicates the Control word is produced from information in the entitlement control message. The Examiner interprets this to be equivalent to the control information.

In response to Applicant's argument beginning on page 23 with respect to claim 10, "Claim 10 recites the steps of retrieving the stored re-encrypted program mater and the fourth encryption key, decrypting the fourth encryption key using the third encryption key. The Applicants respectfully disagree that Okabe can be modified as suggest by the Office Action". The Examiner disagrees with argument for multiple reasons and notes again the both references should be looked at in combination. Okabe teaches re-encrypting program material with subsequent keys. Akins teaches retrieving encrypted program material using previously utilized keys. See passages col. 7, lines 33-38 of Okabe and col. 6, lines 24-53 of Akins.

In response to Applicant's argument beginning on page 24 with respect to claims 12, 13, 38, and 39, "These claims recite details regarding the purchase of stored programs for replay. The Office Action suggest that these features are disclosed ... but the Applicant disagree. Further, Okabe discloses a paradigm where the program material is paid for and the right to replay it determined before the program material is downloaded. The Applicants believe that this paradigm is antithetical to that of Akins, and hence, there is no motivation to combine". The Examiner again is confused by the interpretation of the Applicant and notes Okabe teaches in col. 7, lines 63-66 that the control information can later be updated. The motivation to combine Okabe and Akins in addition to what is provided below is because they both are directed to the same field of digital rights management and digital content distribution.

In response to Applicant's argument beginning on page 19, with respect to claims 2 and 29 these arguments are persuasive and these claims are noted below as containing allowable subject matter.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1, 28, and 43,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Okabe et al. US Patent No. 6,889,208 (hereinafter '208).

As to independent claim 1, "A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of: (a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data" is taught in '208 col. 7, lines 13-25;

"(b) decrypting the received access control information in a conditional access module releasably coupleable with the receive to produce the first encryption key; (c) decrypting the program material using the first encryption key" is shown in '208 col. 7, lines 33-35;

"(d) re-encrypting the program material according to a second encryption key; and" is disclosed in '208 col. 7, lines 34-38;

the following is not explicitly taught in '208: **"(e) encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; (f) providing the re-encrypted program material and the fourth encryption key for storage"** however '208 teaches "various means to incorporate a means of tracking the number of copies made of the content in col. 3, line 64 through col. 4, line 28; in addition '208 teaches "As shown in FIG. 3, the transfer control data contain four bits ... representing a transfer generation number (a copy generation number) ... Each time transferring or copying contents data is executed, the transfer-source player or apparatus (the copy-source player or apparatus) processes the transferred data or the copied data so that the number represented by the transfer-generation-number data piece is decremented by "1". When the transfer-generation-number data piece reaches "0000", transferring or copying contents data is prohibited. For example, the transfer-source player or apparatus (the copy-source player or apparatus) is disabled by the transfer-generation-number data piece being "0000" in col. 8, line 47 through col. 9, line 3. As well '208 teaches "The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" in col. 7, lines 34-38 it is obvious by the text "other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" that as long as the transfer-generation-number contained in the header is not "000" that a new encryption key will be generated and included in the 'encryption-resultant playback key data'. As well '208 teaches "step S34 subsequent to the step S33 encrypts the primary encryption-resultant playback key data into other secondary encryption-resultant playback key data or third encryption-resultant playback key data in response to the ID of the copy-destination player (the transfer-destination player) 6b. A step S35 following the step S34 transmits the encryption-resultant contents data and the secondary encryption-resultant playback key data (generated by the step S34) to the copy-destination player 6b. The customer's player 6b recovers the original contents data as the customer's player 6a does (see FIG. 9). After the step S35, the current execution cycle of the program segment ends. The customer's player 6a is designed to upload the transfer control data representative of the transfer generation number (the copy generation number) to a host side each time the transfer generation number is updated." in col. 12, lines 25-48, this obviously would mean that each time the transfer generation number, and the encryption-resultant playback key data is updated, another key is generated, i.e. 'fourth encryption key', then fifth, sixth, etcetera.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated by generating a new encryption key. One of ordinary skill in the art would have been motivated to perform such a modification because it is desirable to manage copyright data see '208 (col. 1, lines 39 et seq.) "It is desirable to prevent contents data from being transmitted and downloaded to an illegal customer's player. Even in the case where contents data have been transmitted and downloaded to a legitimate customer's player, it is desirable to manage copying the contents data for copyright".

As to independent claim 28, this claim is directed to the apparatus implementing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claim 43, "further comprising the step of generating the second encryption key in the conditional access module" is taught in '208 col. 7, lines 13-48.

8. **Claims 4-16, 31-42, and 44-46** are rejected under 35 U.S.C. 103(a) as being unpatentable over Okabe et al. US Patent No. 6,889,208 (hereinafter '208) in view of Akins, III et al. U.S. Patent No. 6,560,340 (hereinafter '340).

As to dependent claim 4, the following is not taught in '208: "wherein the conditional access module on a smartcard" however '340 teaches "DHCTSE 627 includes a microprocessor (capable of performing DES), specialized hardware for performing RSA encryption and decryption, and secure memory elements. All of the components of DHCTSE 627 are contained in a single tamper-proof package, such as a package that upon attempting to access the information contained within the information is destroyed. Only the components of DHCTSE 627 have access to the information stored in the secure memory elements. Any attempt by a user to gain access to any of the parts of DHCTSE 627 renders DHCTSE 627 unusable and its contents unreadable. DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a "smart card" in col. 21, lines 1-14.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include an improved means of distributing content data. One of ordinary skill in the art would have been motivated to perform such a modification because more flexible means are needed to distribute data see '340 (col. 2, lines 60 et seq.) "Thus, the service distribution organizations require access restrictions which are both more secure and more flexible than those in conventional systems.

As to dependent claim 5, "wherein the access control information further comprises metadata describing at least one right for the program material" however '340 teaches col. 4, lines 50-61. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 6, "further comprising the step of generating the second encryption key at least in part from the metadata" however '340 teaches col. 4, lines 50-61. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 7, "wherein steps (b)-(f) are performed in response to a pre-buy Message" however '340 teaches in col. 12, lines 39-67. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 8, "wherein the access control information further comprises metadata describing at least one right for the program material and the method further comprises the step of: generating replay right data from the metadata" however '340 teaches in col. 31, lines 7-24. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 9, "wherein the replay right dam is further generated from pre-buy data" however '340 teaches in col. 31, lines 7-24. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 10, "further comprising the steps of retrieving the stored re-encrypted program material and the fourth encryption key; decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and decrypting the re-encrypted material using the second encryption key" however '340 teaches in col. 6, lines 24-53. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 11, "wherein the step of decrypting the fourth encryption key using the third encryption key to produce the second encryption key is performed in response to a subscriber request to access the program material" however '340 teaches in col. 30, lines 38-67. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 12, "wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the method further

comprises the steps of; generating replay right data from the metadata; accepting the buy data; comparing the buy data with the replay right data; and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data" however '340 col. 12, line 56 through col. 13, line 39. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 13, "wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein: the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata sued the pie-buy message in the smartcard; and the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data arid the replay right data tire performed in the smartcard" however '340 teaches in col. 21, lines 1-40. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 14, "wherein the re-encrypted program material and the fourth encryption key ate stored on a media storage device" however '340 teaches in col. 7, lines 49-55. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 15, "wherein the control data is temporally-variant" however '340 teaches in col. 28, line 43 through col. 29, line 39. The motivation to combine '340 and '208 is the same as stated above in claim 4.

As to dependent claim 16, "wherein the temporally-variant control data associates an expiration time with the program material" however '340 col. 28, line 43 through col. 29, line 39.

As to dependent claim 44, "wherein the access control information further comprise metadata and the method further comprises the step of generating the second encryption key at least in part from metadata" however '340 teaches generating keys from the metadata received in col. 4, lines 50-61.

As to dependent claim 45, "further comprising the step of: augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" however '340 teaches using the metadata received to update the control information in col. 4, lines 50-61.

As to dependent claim 46, "wherein the access control information further comprises metadata describing at least one right for the program material and the method further comprises the step of : augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" however '340 teaches the metadata consist of program access rights and that these access rights can be used before encryption in col. 4, lines 50-61.

As to dependent claims 31-42, these claims contain substantially similar subject matter as claims 4-16, and 44-46; therefore they are rejected along similar rationale.

9. **Claims 17-27 and 47-50** are rejected under 35 U.S.C. 103(a) as being unpatentable over '208 in view of Akins, III et al. U.S. Patent No. 6,560,340 (hereinafter '340).

As to independent claim 17, "An apparatus for: storing program material encrypted according to a first encryption key for replay, comprising: a conditional access module, for accepting encrypted access control information including the first encryption key" is taught in '208 col. 7, lines 13-25;

"the control access module comprising a first decryption module, for decrypting the access control information to produce the first encryption key" is shown in '208 col. 7, lines 33-35;

"a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and a second decryption module for decrypting the fourth encryption key to produce the second encryption key" however '208 teaches "various means to incorporate a means of tracking the number of copies made of the content in col. 3, line 64 through col. 4, line 28; in addition '208 teaches "As shown in FIG. 3, the transfer control data contain four bits ... representing a transfer generation number (a copy generation number) ... Each time transferring or copying contents data is executed, the transfer-source player or apparatus (the copy-source player or apparatus) processes the transferred data or the copied data so that the number represented by the transfer-generation-number data piece is decremented by "1". When the transfer-generation-number data piece reaches "0000", transferring or copying contents data is prohibited. For example, the transfer-source player or apparatus (the copy-source player or apparatus) is disabled by the transfer-generation-number data piece being "0000" in col. 8, line 47 through col. 9, line 3. As well '208 teaches "The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" in col. 7, lines 34-38 it is obvious by the text "other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" that as long as the transfer-generation-number contained in the header is not "000" that a new encryption key will be generated and included in the 'encryption-resultant playback key data'. As well '208 teaches "step S34 subsequent to the step S33 encrypts the primary encryption-resultant playback key data into other secondary encryption-resultant playback key data or third encryption-resultant playback key data in response to the ID of the copy-destination player (the transfer-destination player) 6b. A step S35 following the step S34 transmits the encryption-resultant contents data and the secondary encryption-resultant playback key data (generated by the step S34) to the copy-destination player 6b. The customer's player 6b recovers the original contents data as the customer's player 6a does (see FIG. 9). After the step S35, the current execution cycle of the program segment ends. The customer's player 6a is designed to upload the transfer control data representative of the transfer generation number (the copy generation number) to a host side each time the transfer generation number is updated." in col. 12, lines 25-48, this obviously would mean that each time the transfer generation number, and the encryption-resultant playback key data is updated, another key is generated, i.e. 'fourth encryption key', then fifth, sixth, etcetera.

the following is not explicitly taught in '208:

"and temporally-variant control data" however '340 teaches that the control data can contain information that varies with data or time in col. 28, line 43 through col. 29, line 39.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include an improved means of distributing content data. One of ordinary skill in the art would have been motivated to perform such a modification because more flexible means are needed to distribute data see '340 (col. 2, lines 60 et seq.) "Thus, the service distribution organizations require access restrictions which are both more secure and more flexible than those in conventional systems.

As to dependent claim 18, further comprising: a tuner, communicatively coupleable to the conditional access module for receiving the encrypted access control information and the program material encrypted according to a first encryption key" is shown in '208 col. 6, lines 34-48 (Note tuner is considered equivalent to a communication device that communicates with a satellite);

"a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module; a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key" is disclosed in '208 col. 3, line 64 through col. 4, line 28.

As to dependent claim 19, "wherein the conditional access module further comprises: a pre-buy module, for controlling the first decryption module" however '340 teaches in col. 12, line 56 through col. 13, line 14. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 20, "wherein the access control information further comprises metadata describing at least one right for the program material" however '340 teaches the metadata distributing program access rights in col. 31, lines 7-24. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 21, "wherein pre-buy module generates replay right data from the metadata" however '340 teaches the use of impulse pay per view message, the pay per view messages are received by the set top box, which obviously is the 'pre-buy module' in col. 12, lines 39-67. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 22, "further comprising a buy module, communicatively coupled to the pre-buy module" " however '340 teaches the use of impulse pay per view message, the pay per view messages are received by the set top box, which obviously is the 'pre-buy module' in col. 12, lines 39-67. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 23, "wherein the buy module comprises: a purchase module; for accepting buy data, and comparing the buy data and the replay right data from the pre-buy module; and a control module for controlling the second decryption module based on the comparison between the buy data and the replay right data" however '340 teaches that the messages receive works with the delivery system and entitlement agents in col. 13, lines 14-54. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 24, "further comprising a billing module, for recording the buy data" however '340 teaches the entitlement agent responds to the FPM by adjusting its billing as required in col. 40, lines 2-5. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 25, "wherein the second encryption key is stored in the conditional access module" is taught in '208 col. 7, lines 13-38.

As to dependent claim 26, "wherein the third encryption key is stored in the conditional access module" is shown in '208 col. 7, lines 13-38.

As to dependent claim 27, "wherein the conditional access module is releaseably communicative coupleable to: a tuner for receiving the encrypted access control information and the program material encrypted according to a first encryption key" is taught in '208 col. 6, lines 33-48;

"a third decryption module, for decrypting the program material using the first encryption key from the conditional access module a second encryption module, for re-encrypting the decrypted program material according to the key" is shown in '208 col. 7, lines 13-48;

"and a media storage device" is disclosed in '208 col. 6, lines 49-67.

As to dependent claim 47, "wherein the conditional access module generates the second encryption key at least in part from the metadata" however '340 teaches in col. 4, lines 50-61. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 48, "wherein the access control information further comprises a metadata and the conditional access module generated the second encryption key at least in part from the metadata" however '340 teaches in col. 4, lines 50-61.

As to dependent claim 49, "wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" is taught in '208 col. 7, lines 13-25.

As to dependent claim 50, "wherein the access control information further comprises metadata, and wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" however '340 teaches in col. 4, lines 50-61. The motivation to combine '208 and '340 is the same as stated above in claim 17.

Allowable Subject Matter

10. **Claims 2 and 29,** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The prior art of record, Okabe et al. introducing a contents sale system where contents are encrypted for playback along with playback key data and the prior art of record Akins et al. introducing a conditional access to services system for a cable television system.

The prior art of record, Okabe or Okabe in view of Akins fail to anticipate or render Applicant's particular feature that

"the encrypted access control information including a first encryption key and temporally-variant (time varying) control data ... modifying the temporally-variant control data to generate temporally-invariant control data; re-encrypting the access control data information including the temporally-invariant control data; ... to a second encryption key; encrypting the second encryption key according to a third encryption key to produce a fourth encryption key"

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 10:00 am to 6:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran

Ellen Tran
Patent Examiner
Technology Center 2134
9 January 2007